UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/711,323	11/09/2000	Alfonso de Jesus Valdes	10454-014002	6879

52197 7590 02/26/2009

PATTERSON & SHERIDAN, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
02/26/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/711,323	VALDES ET AL.	
	Examiner	Art Unit	
	ARAVIND K. MOORTHY	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 10-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 10-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 11 December 2008.

2. Claims 1-5 and 10-12 are pending in the application.

3. Claims 1-5 and 10-12 have been rejected.

4. Claims 6-9 and 13 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11 December 2008 has been entered.

Response to Arguments

6. Regarding the Applicant's arguments filed 12 May 2008, with respect to rejection made under 35 U.S.C. 101, have been fully considered but they are not persuasive.

On page 6, the applicant argues that since the claimed executable program is contained on a computer readable storage medium, the executable program is "structurally and functionally interrelated" to the computer readable storage medium, and, as such, is statutory.

The examiner respectfully disagrees. After a careful review of the specification, the examiner asserts that the applicant has not shown that the computer readable medium is hardware. The examiner has found no support of a “computer readable storage medium

Regarding the prior art, the Applicant's arguments with respect to claims 1-5 and 10-12 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 10-12 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Independent claim 10 is directed towards a computer readable storage medium containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system. Independent claim 11 is directed towards a computer readable storage medium containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised. Independent claim 12 is directed towards a computer readable medium containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised. When nonfunctional descriptive material is recorded on some computer-readable medium, in a computer or on an electromagnetic carrier signal, it is not statutory since no requisite functionality is present to satisfy the practical application requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored in a computer-readable medium, in a computer, on an electromagnetic carrier signal does not make it statutory. See Diehr, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in Benson were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer."). Such a result would exalt form over substance. In re Sarkar, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978)

("[E]ach invention must be evaluated as claimed; yet semantogenic considerations preclude a determination based solely on words appearing in the claims. In the final analysis under Sec. 101, the claimed invention, as a whole, must be evaluated for what it is.") (quoted with approval in Abele, 684 F.2d at 907, 214 USPQ at 687). See also In re Johnson, 589 F.2d 1070, 1077, 200 USPQ 199, 206 (CCPA 1978) ("form of the claim is often an exercise in drafting").

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 10-12 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Independent claims 10-12 all recite a "computer readable storage medium". However, after a careful review of the specification, the examiner has found no support in the applicant's specification for a "computer readable storage medium".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-5 and 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baba U.S. Patent No. 7,051,369 B1 in view of Fox et al U.S. Patent No. 7,096,502 B1 (hereinafter Fox).

As to claims 1 and 3, Baba discloses a method for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by of the intrusion detection system, the method comprising the steps of:

(a) transmitting (sensor sends attack data to the firewall through the director 6) to the first sensor (i.e. firewall 2) information (i.e. first-type attack data) [column 13 line 64 to column 14 line 3] about a belief state of the second sensor (i.e. firewall 2), the belief state of the second sensor indicating a state (i.e. attack data) of at least one system resource or service directly monitored by the second sensor [column 13 line 64 to column 14 line 3]; and

(b) adjusting a prior belief state of the first sensor (i.e. The director, which has been supplied with the detected first-type attack data from the sensor, rewrites the filter setting file of the firewall in order to prevent IP packets having the same

source IP addresses at the source IP addressees contained in the detected first-type attack data from entering the LAN for a predetermined time) [column 13 line 64 to column 14 line 3], the belief state of the first sensor indicating a state of at least one system resource or service directly monitored by the first sensor, the adjusting is based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to suspicious activity in the intrusion detection system is improved [column 14, lines 8-21].

Baba does not teach that the firewall and sensor are probabilistic sensors. Baba does not teach the sensor sending a probabilistic belief to the firewall.

Fox teaches that DPL (decision programming language) is a decision support software package that facilitates the modeling of complex decisions. It allows a user to incorporate uncertainty and flexibility into a decision process. DPL provides a graphical interface for building a model, and performs analyses on the model. DPL-f contains the functionality built into DPL and provides a graphic interface for fault tree construction. This feature allows the modeler to create fault trees and incorporate them into DPL models. DPL-f also contains unique analytic tools. These tools include the ability to calculate explicitly the probability of any event in the tree and perform fault tree-specific types of sensitivity analysis. DPL-f provides an interface for incorporating time series into a model. This allows a modeler to account for devaluation, capital growth or other time-bearing quantities without changing the structure of the model. DPL-f provides RAM with additional capabilities for rapid fault tree construction, libraries of embedded fault trees, an expert opinion generation system, enumeration and ordering of cut sets and a graphical portrayal of risk over time.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba so that the sensors (firewall and sensor) would have had a decision support software package that facilitates the modeling of complex decisions. It would have allowed a user to incorporate uncertainty and flexibility into a decision process. There would have been a graphic interface and analytic tools.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba by the teaching of Fox because it provides integration of the information and the resulting informed assessments available by applying multiple tools that produce a more robust and accurate picture of a system's security posture. These results can facilitate more informed system design decisions, providing a framework for alternative evaluation and comparison [column 3, lines 3-8].

As to claim 2, Baba teaches that the first sensor and the second sensor are different types of sensors (i.e. Baba discloses firewall 2 and sensor 5. The firewall has a filter setting file prescribing what types of IP packets are inhibited from entering the LAN. The sensor functions as an attack detecting means) [column 12, lines 15-36].

As to claim 4, Baba discloses a method of reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting (sensor sends attack data to the firewall through the director 6) to the first sensor (i.e. firewall 2) all or part of a belief (i.e. first-type attack data) [column 13 line 64 to column 14 line 3] of the second sensor (i.e.

firewall 2) regarding an apparent normal, degraded or compromised state (i.e. attack data would be a compromised state) of a resource directly monitored by the second sensor [column 13 line 64 to column 14 line 3]; and

(b) adjusting a belief state of the first sensor, the belief state of the first sensor indicating an apparent normal, degraded or compromised sate of a resource directly monitored by the first sensor (i.e. The director, which has been supplied with the detected first-type attack data from the sensor, rewrites the filter setting file of the firewall in order to prevent IP packets having the same source IP addresses at the source IP addressees contained in the detected first-type attack data from entering the LAN for a predetermined time) [column 13 line 64 to column 14 line 3], so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system (i.e. If the director is not supplied with detected first-type data before the predetermined time, then the director cancels the blocking of IP packets from the source IP addressed of the detected first-type attack data against entry into the LAN) [column 14, lines 16-21].

Baba does not teach that the firewall and sensor are probabilistic sensors. Baba does not teach the sensor sending a probabilistic belief to the firewall.

Fox teaches that DPL (decision programming language) is a decision support software package that facilitates the modeling of complex decisions. It allows a user to incorporate uncertainty and flexibility into a decision process. DPL provides a graphical interface for building a model, and performs analyses on the model. DPL-f contains the functionality built

into DPL and provides a graphic interface for fault tree construction. This feature allows the modeler to create fault trees and incorporate them into DPL models. DPL-f also contains unique analytic tools. These tools include the ability to calculate explicitly the probability of any event in the tree and perform fault tree-specific types of sensitivity analysis. DPL-f provides an interface for incorporating time series into a model. This allows a modeler to account for devaluation, capital growth or other time-bearing quantities without changing the structure of the model. DPL-f provides RAM with additional capabilities for rapid fault tree construction, libraries of embedded fault trees, an expert opinion generation system, enumeration and ordering of cut sets and a graphical portrayal of risk over time.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba so that the sensors (firewall and sensor) would have had a decision support software package that facilitates the modeling of complex decisions. It would have allowed a user to incorporate uncertainty and flexibility into a decision process. There would have been a graphic interface and analytic tools.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba by the teaching of Fox because it provides integration of the information and the resulting informed assessments available by applying multiple tools that produce a more robust and accurate picture of a system's security posture. These results can facilitate more informed system design decisions, providing a framework for alternative evaluation and comparison [column 3, lines 3-8].

As to claim 5, Baba discloses a method of enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection

system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting (sensor sends attack data to the firewall through the director 6) to the first sensor (i.e. firewall 2) all or part of a belief (i.e. first-type attack data) [column 13 line 64 to column 14 line 3] state of the second sensor regarding an existence or validity of services (i.e. determines if a Syn-flood attack has occurred) [column 14, lines 47-55] supported on computer system resources directly monitored by the second sensor (i.e. firewall 2) [column 13 line 64 to column 14 line 3]; and

(b) adjusting a belief state of the first sensor (i.e. The director, which has been supplied with the detected first-type attack data from the sensor, rewrites the filter setting file of the firewall in order to prevent IP packets having the same source IP addresses at the source IP addressees contained in the detected first-type attack data from entering the LAN for a predetermined time) [column 13 line 64 to column 14 line 3], the belief state of the first sensor indicating an existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system (i.e. Firewall is supplied with attack data regarding a SYN attack.) [column 15, lines 31-50].

Baba does not teach that the firewall and sensor are probabilistic sensors. Baba does not teach the sensor sending a probabilistic belief to the firewall.

Fox teaches that DPL (decision programming language) is a decision support software package that facilitates the modeling of complex decisions. It allows a user to incorporate uncertainty and flexibility into a decision process. DPL provides a graphical interface for building a model, and performs analyses on the model. DPL-f contains the functionality built into DPL and provides a graphic interface for fault tree construction. This feature allows the modeler to create fault trees and incorporate them into DPL models. DPL-f also contains unique analytic tools. These tools include the ability to calculate explicitly the probability of any event in the tree and perform fault tree-specific types of sensitivity analysis. DPL-f provides an interface for incorporating time series into a model. This allows a modeler to account for devaluation, capital growth or other time-bearing quantities without changing the structure of the model. DPL-f provides RAM with additional capabilities for rapid fault tree construction, libraries of embedded fault trees, an expert opinion generation system, enumeration and ordering of cut sets and a graphical portrayal of risk over time.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba so that the sensors (firewall and sensor) would have had a decision support software package that facilitates the modeling of complex decisions. It would have allowed a user to incorporate uncertainty and flexibility into a decision process. There would have been a graphic interface and analytic tools.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba by the teaching of Fox because it provides integration of the information and the resulting informed assessments available by applying multiple tools that produce a more robust and accurate picture of a system's security posture.

These results can facilitate more informed system design decisions, providing a framework for alternative evaluation and comparison [column 3, lines 3-8].

As to claim 10, Baba discloses a computer readable storage medium containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, where the program performs the steps of:

> (a) transmitting (sensor sends attack data to the firewall through the director 6) to the first sensor (i.e. firewall 2) information about a belief (i.e. first-type attack data) [column 13 line 64 to column 14 line 3] state of the second sensor (i.e. firewall 2), the belief state of the second sensor indicating a state of at least one system resource or service (i.e. determines if a Syn-flood attack has occurred) [column 14, lines 47-55] directly monitored by the second sensor [column 13 line 64 to column 14 line 3]; and
>
> (b) adjusting a belief state of the first sensor (i.e. The director, which has been supplied with the detected first-type attack data from the sensor, rewrites the filter setting file of the firewall in order to prevent IP packets having the same source IP addresses at the source IP addressees contained in the detected first-type attack data from entering the LAN for a predetermined time) [column 13 line 64 to column 14 line 3], the belief state of the first sensor indicating a state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity

of the first sensor to suspicious activity in the intrusion detection system is improved [column 14, lines 8-21].

Baba does not teach that the firewall and sensor are probabilistic sensors. Baba does not teach the sensor sending a probabilistic belief to the firewall.

Fox teaches that DPL (decision programming language) is a decision support software package that facilitates the modeling of complex decisions. It allows a user to incorporate uncertainty and flexibility into a decision process. DPL provides a graphical interface for building a model, and performs analyses on the model. DPL-f contains the functionality built into DPL and provides a graphic interface for fault tree construction. This feature allows the modeler to create fault trees and incorporate them into DPL models. DPL-f also contains unique analytic tools. These tools include the ability to calculate explicitly the probability of any event in the tree and perform fault tree-specific types of sensitivity analysis. DPL-f provides an interface for incorporating time series into a model. This allows a modeler to account for devaluation, capital growth or other time-bearing quantities without changing the structure of the model. DPL-f provides RAM with additional capabilities for rapid fault tree construction, libraries of embedded fault trees, an expert opinion generation system, enumeration and ordering of cut sets and a graphical portrayal of risk over time.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba so that the sensors (firewall and sensor) would have had a decision support software package that facilitates the modeling of complex decisions. It would have allowed a user to incorporate uncertainty and flexibility into a decision process. There would have been a graphic interface and analytic tools.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba by the teaching of Fox because it provides integration of the information and the resulting informed assessments available by applying multiple tools that produce a more robust and accurate picture of a system's security posture. These results can facilitate more informed system design decisions, providing a framework for alternative evaluation and comparison [column 3, lines 3-8].

As to claim 11, Baba discloses a computer readable storage medium containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by of the intrusion detection system, where the program performs the steps of:

(a) transmitting (sensor sends attack data to the firewall through the director 6) to the first sensor (i.e. firewall 2) all or part of a belief (i.e. first-type attack data) [column 13 line 64 to column 14 line 3] of the second sensor (i.e. firewall 2) regarding an apparent normal, degraded or compromised state (i.e. attack data would be a compromised state) of a resource directly monitored by the second sensor [column 13 line 64 to column 14 line 3]; and

(b) adjusting a belief state of the first sensor, the belief state of the first sensor indicating an apparent normal (i.e. The director, which has been supplied with the detected first-type attack data from the sensor, rewrites the filter setting file of the firewall in order to prevent IP packets having the same source IP addresses at the source IP addressees contained in the detected first-type attack

> data from entering the LAN for a predetermined time) [column 13 line 64 to column 14 line 3], degraded or compromised state of a resource directly monitored by the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system (i.e. If the director is not supplied with detected first-type data before the predetermined time, then the director cancels the blocking of IP packets from the source IP addressed of the detected first-type attack data against entry into the LAN) [column 14, lines 16-21].

Baba does not teach that the firewall and sensor are probabilistic sensors. Baba does not teach the sensor sending a probabilistic belief to the firewall.

Fox teaches that DPL (decision programming language) is a decision support software package that facilitates the modeling of complex decisions. It allows a user to incorporate uncertainty and flexibility into a decision process. DPL provides a graphical interface for building a model, and performs analyses on the model. DPL-f contains the functionality built into DPL and provides a graphic interface for fault tree construction. This feature allows the modeler to create fault trees and incorporate them into DPL models. DPL-f also contains unique analytic tools. These tools include the ability to calculate explicitly the probability of any event in the tree and perform fault tree-specific types of sensitivity analysis. DPL-f provides an interface for incorporating time series into a model. This allows a modeler to account for devaluation, capital growth or other time-bearing quantities without changing the structure of the model. DPL-f provides RAM with additional capabilities for rapid fault tree construction,

libraries of embedded fault trees, an expert opinion generation system, enumeration and ordering of cut sets and a graphical portrayal of risk over time.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba so that the sensors (firewall and sensor) would have had a decision support software package that facilitates the modeling of complex decisions. It would have allowed a user to incorporate uncertainty and flexibility into a decision process. There would have been a graphic interface and analytic tools.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba by the teaching of Fox because it provides integration of the information and the resulting informed assessments available by applying multiple tools that produce a more robust and accurate picture of a system's security posture. These results can facilitate more informed system design decisions, providing a framework for alternative evaluation and comparison [column 3, lines 3-8].

As to claim 12, Baba discloses a computer readable storage medium containing an executable program for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting (sensor sends attack data to the firewall through the director 6) to the first sensor (i.e. firewall 2) all or part of a belief (i.e. first-type attack data) [column 13 line 64 to column 14 line 3] state of the second sensor (i.e. firewall 2) regarding an existence or validity of services (i.e. determines if a

Syn-flood attack has occurred) [column 14, lines 47-55] supported on computer system resources directly monitored by the second sensor [column 13 line 64 to column 14 line 3]; and

(b) adjusting a belief state of the first sensor (i.e. The director, which has been supplied with the detected first-type attack data from the sensor, rewrites the filter setting file of the firewall in order to prevent IP packets having the same source IP addresses at the source IP addressees contained in the detected first-type attack data from entering the LAN for a predetermined time) [column 13 line 64 to column 14 line 3], the belief state of the first sensor indicating an existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent service or resource appears suspicious to the intrusion detection system (i.e. Firewall is supplied with attack data regarding a SYN attack.) [column 15, lines 31-50].

Baba does not teach that the firewall and sensor are probabilistic sensors. Baba does not teach the sensor sending a probabilistic belief to the firewall.

Fox teaches that DPL (decision programming language) is a decision support software package that facilitates the modeling of complex decisions. It allows a user to incorporate uncertainty and flexibility into a decision process. DPL provides a graphical interface for building a model, and performs analyses on the model. DPL-f contains the functionality built into DPL and provides a graphic interface for fault tree construction. This feature allows the modeler to create fault trees and incorporate them into DPL models. DPL-f also contains unique analytic tools. These tools include the ability to calculate explicitly the probability of any event

in the tree and perform fault tree-specific types of sensitivity analysis. DPL-f provides an interface for incorporating time series into a model. This allows a modeler to account for devaluation, capital growth or other time-bearing quantities without changing the structure of the model. DPL-f provides RAM with additional capabilities for rapid fault tree construction, libraries of embedded fault trees, an expert opinion generation system, enumeration and ordering of cut sets and a graphical portrayal of risk over time.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba so that the sensors (firewall and sensor) would have had a decision support software package that facilitates the modeling of complex decisions. It would have allowed a user to incorporate uncertainty and flexibility into a decision process. There would have been a graphic interface and analytic tools.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Baba by the teaching of Fox because it provides integration of the information and the resulting informed assessments available by applying multiple tools that produce a more robust and accurate picture of a system's security posture. These results can facilitate more informed system design decisions, providing a framework for alternative evaluation and comparison [column 3, lines 3-8].

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ARAVIND K. MOORTHY whose telephone number is (571)272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431